RFID - INES

la police totale

Les nanos,
ça sert aussi au mouchardage électronique

RFID : la police totale

RFID : vous avez entendu cet acronyme - ou étiquettes "intelligentes", "smart tags", puces à radiofréquence, transpondeurs. Mais que sont-elles exactement ? À quoi servent-elles ? Comment fonctionnent-elles ? Saviez-vous que 2006 était l'année de leur entrée massive dans les entreprises ? Qu'on les injecte à nos animaux ? Qu'elles vous traquent déjà ? Saviez-vous qu'elles sont une des premières applications des nanotechnologies, et l'une des spécialités locales, entre le "Pôle de traçabilité" de Valence et le "Pôle Minalogic" de l'Isère ? Savez-vous que dans quatre ans, sauf révolte, les mouchards électroniques infesteront 30 milliards d'objets – cinq par être humain, PapouEs comprisES ? Non ? Alors découvrons ensemble ce bijou de *reality*-science.

Histoire vraie.

Au pré avec sa mère, le poulain de trois jours tangue sur ses pattes. La seringue pénètre sous la peau du cou. Injection rapide et indolore. Le vétérinaire vérifie son lecteur portable : le numéro d'identification X0723A s'inscrit à l'écran, la puce est opérationnelle. Grâce à l'interface sans fil Bluetooth, le lecteur transmet directement à l'ordinateur les données concernant X0723A : date de naissance, sexe, numéro des géniteurs, vaccinations, allaitement, etc. Il sera désormais simple, en consultant les bases de données, d'assurer un suivi sanitaire rigoureux, de vérifier qui est le propriétaire, et, en le scannant avec un lecteur portable, d'identifier à tout moment X0723A.

L'animal est entré dans le système, il a le droit d'exister.

Ceci n'est pas du roman, mais une compilation de plaquettes publicitaires comme celle de la société française IER, fournisseur de "*solutions complètes pour l'identification électronique des animaux*". AmiEs citadinEs, vous ignorez sans doute ce que les agriculteurs, éleveurs et ruraux savent déjà : les RFID envahissent nos vies pour les contrôler. Non seulement en transformant les animaux en machines communicantes, mais en implantant dans chaque chose, chaque être, un mini-mouchard électronique. Mais pas de panique : vous n'avez rien à vous reprocher.

"Sans contact" mais avec mouchard

Qu'est-ce que c'est que ces RFID – *Radio-Frequency Identification* en anglais ? La traduction sur quelques millimètres carrés d'un désir totalitaire de tout suivre, pister, détecter, contrôler, surveiller électroniquement.

Même des arbres, oui.

La chose ressemble à une mini-étiquette (d'où son nom d'étiquette "intelligente", ou "smart tag") et se compose d'une puce et d'une antenne. Chaque étiquette est unique, donc distingue l'objet ou la personne qui la porte parmi tous les autres, et est lisible à distance, à travers l'épaisseur de la peau, d'un emballage, de l'écorce, d'une couche de neige épaisse, etc.
Ça vous rappelle quelque chose ? Oui, Navigo, votre pass de métro parisien, ou Avan'Tag, pour le tram grenoblois, que vous ne sortez plus de votre sac pour valider. Ou le passe sans contact des autoroutes qui débite votre compte. Ou encore le forfait de ski de Chamrousse, validé lui aussi à distance dans la queue du télésiège. Trop pratique. À condition d'admettre que chacun de vos déplacements soit enregistré – date, heure, trajet, temps de parcours, etc.
C'est l'intérêt principal des RFID pour leurs utilisateurs : recueillir et stocker des millions de données – une richesse dans la société de l'information ; une source de pouvoir dans la société de la domination.
Comme on dit au labo Auto-ID du Massachussetts Institute of Technology (MIT): *"Mettez une étiquette RFID sur une canette de Coca ou un essieu de voiture, et soudain un ordinateur peut la "voir". Mettez des étiquettes sur chaque canette et chaque essieu et soudain le monde change (…) Le centre Auto-ID conçoit, construit, teste et déploie une infrastructure globale qui permettra aux ordinateurs d'identifier tout objet instantanément n'importe où dans le monde."*[1]

D'autres exemples ? Le portable de Nokia avec lecteur RFID pour inventorier les objets "taggés" autour de nous et transmettre ces données à distance[2]. Le dispositif "Person Tracking Unit" d'IBM permettant de scanner les étiquettes sur les éléments d'une foule pour suivre les mouvements dans les lieux publics. Les billets de la Coupe du Monde 2006 avec mouchard pour faciliter le suivi des supporters. Dans les bibliothèques françaises on équipe les livres : l'enregistrement de vos emprunts se fait au passage du portique de sortie. Dans des collèges américains on contrôle la présence et le comportement des élèves par leur carte électronique[3]. Certaines communes, dont Paris, pucent leurs arbres pour mieux les *gérer*.
Mais encore : suivi des bagages dans les aéroports ; identification des véhicules, des produits de luxe et des médicaments (contre la contrefaçon) ; ouverture contrôlée des portes électroniques ; remplacement des badges ; passeports, visas et cartes d'identité électroniques ; gestion des livraisons pour l'armée ; traçabilité alimentaire ; puçage des animaux. Et des humainEs - on y vient.
Rien sur cette planète ne doit échapper à la frénésie de la traçabilité. Le lobbying des fabricants de puces a fait son oeuvre : *"Le marché est*

1 cf http://www.autoidlabs.org/
2 http://www.rfidjournal.com/article/articleview/834/1/13/
3 cf http://www.incomcorporation.com/, affaire du collège californien qui impose les RFID à ses élèves

considérable et le pays par la voix de Michèle Alliot-Marie, ministre de la Défense et de François Loos, ministre délégué à l'Industrie va prochainement assouplir la réglementation en vigueur. L'objectif est surtout de permettre son développement et son utilisation sur l'ensemble du territoire, y compris les DOM-TOM."[4]

Dans la grande distribution, les étiquettes "intelligentes" permettent de suivre les produits de l'usine à la déchetterie, en passant par le transport, le stockage, l'achat, et de lutter contre les vols – pardon, les "démarques inconnues".

Avis aux chapardeuses/eurs : la petite taille des RFID permet de les dissimuler dans le tissu des vêtements, dans le papier des passeports, dans le corps même des objets. Début février 2006, Hitachi a présenté la plus petite puce RFID du monde : 0,15 mm de côté et 7,5 µm d'épaisseur. Invisible, indétectable, sauf par la machine et celleux qui pilotent la machine. Sachez-le avant de remplir vos poches (quoique le papier aluminium semble perturber la transmission par radiofréquences. Bref.).

Wal-Mart aux Etats-Unis a imposé les RFID à ses principaux fournisseurs depuis 2005, imité par Tesco et Marks & Spencer en Grande-Bretagne, Metro en Allemagne. Ce dernier expérimente depuis 2003 le "magasin du futur"[5]. Votre caddie, équipé d'un écran informatique et d'un lecteur, enregistre chaque produit et vous assiste dans vos courses, idiotE comme vous êtes (localisation des produits dans les rayons, conseils, promos, etc). L'objectif est d'éliminer les humainEs aux caisses, le chariot débitera votre compte. À la sortie vous pouvez désactiver les RFID. Si vous avez le temps de les passer une par une devant une nouvelle machine, et si vous y pensez. Sinon, elles signaleront votre présence dès que vous passerez devant un lecteur. Et en France ? Carrefour a signé en février 2006 un contrat avec le fabricant Checkpoint Systems pour installer des lecteurs RFID dans 179 hypermarchés.



"Le manteau marque Tex taille 42, n°987328765, acheté le 12/11/06 à 17h08 à Carrefour-Meylan, payé par la carte bancaire de Gisèle Chabert de Grenoble, est passé dans le champ du lecteur de Grand-Place aujourd'hui à 8h42, hier à 11h20, et lundi dernier à 9h05. Il est associé au livre "30 recettes pour maigrir en famille" emprunté à la bibliothèque du centre-ville par Gisèle Chabert, et à la carte Avan'Tag de Sonia Chabert, etc"

4 http://www.generation-nt.com/actualites/12098/rfid-etudearcep, février 2006

5 cf *T&T*, magazine de la traçabilité, n°1, octobre 2005

Notice technique
Comment les mouchards RFID nous pistent-ils ? En associant une puce et une antenne. La puce possède son propre identifiant, qui la distingue de toutes les autres. L'antenne transmet par radiofréquences les informations contenues dans la puce (pour les étiquettes "passives"), ou enregistre de nouvelles informations au fil du temps (étiquettes "actives"). Les passives sont alimentées en énergie par le champ électromagnétique émis par le lecteur, et les actives intègrent une mini-pile qui les rend autonomes. Le lecteur peut être manuel (comme les lecteurs de codes-barres), s'intégrer à un portique (comme aux péages d'autoroute) ou être dissimulé dans l'environnement (mobilier urbain, portes, etc).
Les RFID utilisent quatre bandes de fréquence : moins de 135 kHz (basses fréquences), 13,56 mHz (hautes fréquences), 868-950 mHz (ultra hautes fréquences), 2,45 GHz (micro-ondes). Plus les fréquences sont hautes, plus on peut lire la puce de loin (de quelques centimètres à plusieurs dizaines de mètres).

Historique
L'idée remonte à la fin des années 1940. Les militaires anglais mettent au point un système d'identification longue distance pour distinguer par radar les avions amis des autres (*"Identify : Friend or Foe"*). Un demi-siècle de miniaturisation électronique, de mondialisation des échanges, de crises sanitaires, environnementales et alimentaires étend le concept d'identification à celui de *traçabilité*, désormais appliqué à tout ce que la terre porte d'êtres vivants, de ressources, d'objets. Le premier brevet lié aux RFID date de 1969, déposé aux Etats-Unis par Mario Cardullo[6]. Jusque dans les années 1980 la technologie reste militaire ou dédiée à la sécurité des sites "sensibles", nucléaires entre autres. Ensuite le secteur privé la commercialise pour l'identification du bétail avant d'étendre son usage et de standardiser les équipements.[7]

Dans les laboratoires Auto-ID, créés par le MIT et une centaine de grands groupes (Procter & Gamble, Gillette, Carrefour, Coca, Nestlé, le Département de la Défense américaine), les chercheurEs étudient la création d'un "Internet des objets" pour centraliser les données transmises par les millions de RFID en circulation. Une *toile* qui localisera chaque objet et racontera sa vie - il est passé par là, repassé par ici – et qui permettra aux choses de communiquer entre elles, éliminant enfin l'intervention humaine : frigo qui commande les yaourts, machine à laver qui choisit le programme selon les vêtements, etc.
Feu Mark Weiser, ex-directeur de recherche de Xerox à Palo Alto, nous avait prévenus : *"Les technologies les plus profondément enracinées sont les*

6 Ingénieur qui participa aux programmes de satellites pour la marine
et les communications mobiles (IMARSAT) ; de propulsion des roquettes et des moteurs de lance-missiles dans le cadre du programme Apollo (cf. http://www.nvgc.vt.edu/engineering/Cardullo.htm)
7 *Science & Vie*, avril 2004 et http://www.poletracabilite.com/

technologies invisibles. Elles s'intègrent dans la trame de la vie quotidienne pour ne plus pouvoir en être distinguées."[8]

Et alors ?

Pucer un objet, un animal, une personne, les transforme en machines, faciles à relier entre elles pour créer un réseau total, un *filet* ("net") transmetteur d'informations en continu. Il ne suffisait pas que nous fussions *connectés* et joignables en permanence par téléphone portable, mails, SMS ou Wifi ; avec les RFID nous devenons nous-mêmes des *objets communicants*. Des objets. Que nos maîtres suivent à la trace, dont ils analysent les comportements, contrôlent les mouvements pour mieux les "gérer".

Comme les ordinateurs, nous aurons bientôt chacun une adresse électronique permettant notre localisation permanente. Le projet est à l'étude, breveté sous l'appellation UIAD[9] (Identification Unique des Adresses). *"Le monde est entré depuis quelques années dans la frénésie de donner une adresse, de préférence permanente, non seulement aux objets physiques, aux individus, aux véhicules sur la route, aux animaux, sous prétexte de traçabilité, mais aussi à tous les objets virtuels, que ce soit les messages de type courriel ou SMS, les documents administratifs, les morceaux de musique numérisés ou les micro-esclaves logiciels (…) qui parcourent inlassablement les réseaux en y troquant des micro-informations pour mieux nous servir, voire souvent pour mieux nous espionner."*[10]

Puce policière

Nous pister à travers nos objets est instructif mais incertain. Pour s'assurer que vous êtes passéEs à Grand-Place hier soir, il faut pucer vos papiers d'identité. Les Etats-Unis exigent des étrangers le passeport biométrique et électronique. La France prépare sa carte d'identité électronique (INES) avec des données biométriques dans une puce RFID. Finis les contrôles d'identité humiliants, voici les contrôles d'identité sournois, à distance.

"Grenoble place de la gare le 12/03/08 à 14h11. Manifestation des étudiants. Présence des individus X (carte d'identité n°98729872), Z (carte d'identité n°62902U74), Y (carte de séjour n°87AHE87982) détectée en tête de cortège. Attention, détection de l'individu G (carte d'identité n°816539837) fiché pour participation au fauchage d'un champs d'OGM dans la Drôme le 27/07/07."



---

8 cf Union Internationale des Télécommunications (http://www.itu.int/)

9 cf http//www.uiad.org/

10 cf *"Les technologies de radio-identification (RFID) : enjeux industriels et questions sociétales"*, rapport du Conseil général des technologies de l'information, janvier 2005

Les nostalgiques de Vichy peuvent regretter la lenteur du *progrès* technologique : avec le mouchard électronique, les rafles auraient affiché de meilleurs rendements. Aux opposants des nanotechnologies, illes lanceraient, si la loi actuelle le leur permettait : "*Vous êtes des passéistes, vous voulez retourner à l'étoile Jaune*".

Vous prendrez bien un peu de pâtée industrielle traçabilisée ?
Supposée empêcher les attaques terroristes, la traçabilité doit aussi nous protéger des risques sanitaires. La vache folle a servi d'alibi au puçage des animaux. Etiquetées, codebarrisées, fichées, les bêtes sont désormais implantées au nom de la "sécurité alimentaire".
L'implant électronique est le corollaire de la fabrication industrielle de steacks. Viande sur pattes élevée en usine, alimentée par rations synthétiques, maintenue en survie par antibiotiques, *gérée* par *monitoring* zootechnique, transportée sur des milliers de kilomètres, débitée en morceaux calibrés, fourguée en hypermarchés. *J'ai quand même le droit de savoir ce que je consomme*, réclame la/le pousseuse/eur de caddie, rassuréE par la puce qui trace ses hamburgers de leur naissance au micro-ondes.
Bien entendu la traçabilité ne signale rien d'autre que le progrès fulgurant de *l'insécurité* alimentaire créée par l'industrialisation de l'agriculture. Car des animaux élevés en batterie sont des animaux malades, et des végétaux sous perfusion d'engrais, d'hormones, d'insecticides, etc, sont des végétaux malades. Comment éviter les épidémies chez les porcs, malades de l'élevage industriel ? En les puçant, répond le ministère espagnol de l'Agriculture.[11]
Vous ne voulez pas d'OGM dans vos assiettes ? Vous mangerez des OGM traçabilisés. Nous voilà rassurés. Dans le monde de la techno-agriculture, la traçabilité remplace les prés pour les troupeaux, les sols vivants pour les plantes, la maîtrise de leur travail pour les paysans, la relation consommatrice/teur-productrice/teur.
Si nos légumes du marché sont abîmés, nous en discutons avec la/le productric/teur. Si vous achetez à Carrefour un chili con carne en boîte, dont la viande est née en Allemagne, a grandi en Hollande nourrie par des rations importées d'Amérique Latine, et dont les haricots ont poussé en Italie pour être préparés en Espagne, le tout assaisonné de conservateurs en Belgique, comment retrouver l'origine du germe infectieux ? Grâce à la puce. Ainsi mangeons-nous de la daube authentifiée, ce qui suffit semble-t-il à la/au cochonNE de consommatrice/teur.

Refuser les RFID, c'est refuser la traçabilité et la manipulation du *sentiment* d'insécurité. Nous voulons bien manger ? Boycottons les supermarchés. Associons-nous pour acheter directement.

11 http://www.agrisalon.com/, 07/11/01

De l'animal à l'homme domestique

En 2006 en France, on peut lire, à la page "Pratique" de son quotidien, ce genre de conseil : "*Mieux que le tatouage. La puce est très pratique par rapport au tatouage, car : la pose ne nécessite pas d'anesthésie ; la lecture peut se faire à distance, ce qui est avantageux à l'égard des animaux apeurés ou nerveux ; elle est invisible, infalsifiable et permanente, elle ne risque pas comme le tatouage de s'effacer au fur et à mesure des années. Un outil international. Le fichier sera mondial, l'animal pourra être facilement identifié aux frontières et à l'étranger. Rappelez-vous qu'il est obligatoire que touTEs les chienNEs et chatTEs de plus de 4 mois soient identifiéEs. N'hésitez donc pas à le faire, c'est rapide et sans douleur.*"[12]

Carte d'identité, carte Vitale, fichier automatisé des empreintes digitales, fichier national des empreintes génétiques nous ont accoutuméEs au fichage systématique de la population et à l'électronisation du contrôle. Comme des grenouilles dans l'eau froide nous supportons la hausse progressive de température, sans réaliser qu'elle nous ébouillante aussi sûrement qu'un plongeon dans un bain brûlant. Avec le puçage électronique, voici bientôt les 100°C. On puce d'abord les animaux d'élevage (sécurité alimentaire) les animaux sauvages (lutte contre les trafics), les animaux domestiques ("très pratique"). Ainsi le territoire est-il peu à peu maillé, les lecteurs de RFID implantés partout. Toutes les institutions susceptibles d'avoir à identifier un animal perdu s'équipent : pompierEs, gendarmes, douanierEs, directions des services vétérinaires, refuges, fourrières, ainsi que les 5500 cabinets et cliniques vétérinaires français. Comme le note un ami des bêtes : "*puisque mon chien est toujours avec moi, détecter sa présence, c'est détecter la mienne*". Surtout, pucer nos animaux nous familiarise avec la traçabilité électronique. Vous ne feriez pas à votre chien ce que vous refuseriez qu'on vous fasse, n'est-ce pas ? Comment les enfants dont l'animal est scanné par le véto s'étonneraient-ils de subir le même sort ? Dans vingt ans, l'article du *Daubé* sera republié, "individuE" remplaçant "animal", sans plus émouvoir quiconque que ce "conseil pratique" de 2006.

Refusons de transformer nos animaux en gadgets électroniques, ou nous subirons le même sort.

La société américaine Applied Digital Solutions s'y emploie depuis les années 2000 avec Verichip, sa puce sous-cutanée pour humainEs, à usages multiples : suivi des enfants dont les parents craignent l'enlèvement, patientEs de dizaines d'hôpitaux américains portant *en eux* leur dossier médical numérisé, clientEs branchéEs de boîtes de nuit espagnoles et hollandaises pour payer leurs conso sans sortir de monnaie, employéEs de banque australienNEs obligéEs de se faire scanner le bras pour accéder à leur poste, etc. Sans oublier les mortEs du cyclone Katrina ; les techno-fans qui se font pucer pour sécuriser l'ouverture de leur maison ou de leur voiture ; et les projets multiples de puçage des

12 *Le Daubé*, 10/02/06

malades psychiatriques, des SDF, des enfants dès la naissance[13].
Avertissement au cheptel humain : aujourd'hui une brebis baladeuse trouvée sans puce est conduite à l'équarrissage sans sommation.

Le flicage, c'est bon pour l'emploi

Lectrice/teur, tu trouves ces nouvelles inquiétantes, déprimantes, paralysantes ? Tu te demandes si ces accumulations d'ondes hertziennes (portable, Wifi, RFID, ça commence à faire) menacent ta santé ? Si ces milliards de puces électroniques disséminées dans les décharges ne vont pas polluer plus encore les sols et les nappes phréatiques ? Tu crains pour la liberté et la dignité humaine ? Tu imagines tes contemporainEs conditionnéEs, volontaires pour la servitude électronique ? Ne désespère pas, lecteur, lectrice. Au moins ces sacrifices sont-ils bénéfiques à l'économie locale, et qui sait ? préserveront ton propre emploi dans la cuvette grenobloise.
D'après les études des cabinets spécialisés, le marché RFID doit exploser à partir de 2006, avec des prévisions atteignant 10 à 20 milliards d'objets pucés en 2008[14], et 33 milliards en 2010 contre 1,3 milliards en 2005[15].

Chaque matin des ingénieurEs et technicienNEs iséroiSEs vont au boulot, travailler sur "*des techniques d'impression en phase liquide (…) des circuits électroniques de la puce RFID*"[16] (CEA-Léti) ; sur "*la conception et l'optimisation d'antennes intégrées pour la RFID*"[17] (INPG) ; la fabrication de "*matériaux polymères organiques servant à réaliser les RFID*" (Ciba) ; des "*procédés de gravure dans des résolutions suffisantes pour la production d'électroniques sur substrats souples (antenne RFID, transistors ...)*"[18] (Piolat) ; la "*réalisation d'antennes RFID organiques imprimées*"[19] (Sofileta) ; la conception de "*gammes complètes de produits sans contact RFID*"[20] (Atmel) ; la réalisation des "*premières étiquettes RFID entièrement en plastique*"[21] (Philips) ; le développement d'une "*large gamme d'étiquettes RFID et de produits sans contact*"[22] (STMicroelectronics) ; des "*solutions RFID clé en main*"[23] (Tagproduct) ; la commercialisation de "*l'offre la plus complète du marché dans les domaines de la monétique et du RFID*"[24] (Silicomp). Etc.

Grenoble serait donc *aussi* la capitale des RFID ? "*Le devenir des RFID est au*

13 cf http://www.stoppuce.be/ ou http://www.jameh.org/
14 cf "*Les technologies de radio-identification (RFID) : enjeux industriels et questions sociétales*", rapport du Conseil général des technologies de l'information, janvier 2005
15 *Times*, 19/01/06
16 *L'Usine Nouvelle*, 27/01/05
17 *La lettre de Minatec*, n°9 septembre 2005
18 dossier Minalogic, annexes
19 Idem
20 http://www.atmel.com/ad/wireless/rfid/default.asp
21 http://www.lelectronique.com/actualite/voir.php?news=actu&num=1922
22 http://www.st.com/rfid
23 http://www.tagproduct.com/
24 Inovallée Mag', n°82, septembre 2005

coeur de Minalogic", affirme *Le Daubé*[25] - Minalogic, "pôle de compétitivité mondial" de Grenoble-Isère. Restons modestes, Grenoble est *l'une* des adresses de la RFID française. Comme le dit Gérard-André Dessenne, responsable du développement du Pôle Traçabilité de Valence : *"Nous nous trouvons (…) dans le "coeur" technologique de la France, dans ce carré magique de la RFID constitué par les villes de Grenoble, Valence, Sophia-Antipolis et Aix-en-Provence.*"[26]

Tu vois, lectrice/teur, tu peux te réjouir d'appartenir à la future *continuité urbaine* Genève-Valence (le "Sillon alpin") complotée par nos élus pour 2020. Après tout l'autoroute met Valence à 40 minutes du Polygone scientifique de Grenoble, soit moins que Crolles aux heures de pointe. Puisque nous vivrons bientôt dans la même ville, partageons la fierté d'être du "*carré magique de la RFID*". L'INPG a déjà implanté une de ses écoles à Valence, l'Esisar, qui forme les futurs ingénieurs aux RFID en partenariat avec les industriels. L'Esisar, qui a créé le "Pôle Traçabilité" valentinois avec l'Agence Rhône-Alpes pour la maîtrise des technologies de mesure (ARATEM).

Que peut bien être un "Pôle Traçabilité", demandes-tu ?
"*Un centre d'échanges et de transferts de savoirs,* répond G-A Dessenne. *Il constitue un faisceau de compétences à vocation aujourd'hui nationale et demain européenne, en matière de recherche, de développement, de formation et de transfert vers l'industrie, en particulier en RFID*".[27]
Pressé d'infester nos vies de mouchards, le pôle propose aux entreprises un centre d'essai et de démonstration pour RFID. Extrait du dossier de presse : "*Avec la RFID, la traçabilité peut devenir active et dynamique. Même les plus petits objets peuvent être dotés d'une identité propre et d'un historique précis qui les rend faciles à suivre.*"

De Grenoble à Valence, les ingénieurEs et technicienNEs du carré magique vont chaque matin au boulot, inventer et fabriquer les outils de la surveillance ubiquitaire. Pour rien au monde – surtout pas pour préserver leur liberté et leur dignité – illes ne renonceraient à leurs *recherches*, à leurs *innovations*, à leurs *brevets*, à leur *carrière*. Après elleux, et à cause d'elleux, le déluge de contrôles.

Dites "mouchards verts" plutôt que "mouchards intelligents"
ConscientEs de leur énormité liberticide, chercheurEs et industrielLEs travaillent à *l'acceptabilité* des RFID.
En juillet 2003, le centre Auto-ID du MIT laisse malencontreusement en ligne

25 *Le Daubé,* 12/10/05
26 http://dc.editricetemi.com/ed_temi/dcFr/articolo.jsp?idArt=83
27 Http://www.tracenews.net/

des documents confidentiels. L'association anti-RFID américaine CASPIAN[28] révèle alors que les fabricants de mouchards se font conseiller par l'agence de com' Fleishman-Hillard pour mieux fourguer leurs espions : abandonner le nom "*Smart tags*" pour "*Green Tags*", supposé plus rassurant ; "*positionner la technologie comme étant simplement un code-barre amélioré*", etc. Finalement, les chercheurEs avouent espérer que les consommateurs seront "*apathiques*" et "*se résigneront d'eux-mêmes à l'inévitabilité de la chose*".[29]

À Grenoble, les sociologues des "usages" qui complotent des méthodes pour nous faire accepter l'inacceptable ne pouvaient passer à côté des RFID. Le groupement d'intérêt scientifique "Pegasus" créé en 2003 sur la question des "objets communicants" par le CNRS, l'INPG, l'Université Joseph-Fourier et l'Université Mendès-France compte parmi ses membres de vieilles connaissances : Philippe Mallein et Jean Caelen entre autres[30]. Un des projets qui mobilisent ces pros de la manipulation s'intitule "*Toamutu : Traçabilité des objets et des agents manipulés par des utilisateurs et tests d'usage*". Il s'agit bien sûr d'améliorer les performances des outils de pistage.
"*Objectifs sociétaux : la demande dans la traçabilité des objets est de plus en plus forte (…). Ces produits sont manipulés par de nombreux acteurs au cours de leur cycle de vie, il s'agit de leur donner une nano-mémoire pour qu'ils racontent eux-mêmes cette vie. Ainsi on espère pouvoir retracer leur histoire ainsi que l'histoire qu'ils ont eue avec d'autres objets et agents artificiels ou humains.*"[31]
Le vocabulaire mielleux pour évoquer ces objets dont on raconte l'"histoire" masque mal la duperie. Qui exactement "*espère retracer*" cette histoire qui, au fait, est la nôtre ?

Les RFID sont aux nanotechnologies ce que Terminator est aux OGM : un déclencheur de révolte.
Aussi les chercheurEs en nanos sont-illes prêtEs à tout pour détourner notre attention – déni, mensonge, lâcheté. Interpellé lors d'une émission de France Inter[32] sur les nanotechnologies, Claude Weisbuch, directeur de recherche au CNRS, osa une parade que des journalistes sérieux eussent contrée – mais à France Inter on est courtois avec les invités : les RFID, lâcha Weisbuch, c'est pas nano. "*Les RFID posent des problèmes effectivement d'identification des individus et de contrôle si on met les informations en ligne, si on échange des fichiers, etc, mais les RFID c'est pas nano, simplement parce que pour avoir de*

---

28 Cunsumers against supermarket privacy invasion and numbering, http://www.spychips.com/
29 cf http://transfert.net/a9099/
30 cf *Aujourd'hui le nanomonde* n°3, "*Ideas Lab, la machine à fabriquer des besoins*" sur http://www.piecesetmaindoeuvre.com/
31 "*Objets, agents et environnements communicants*", exposé devant le Conseil scientifique international 2004 (J. Caelen, JP Laurencin)
32 "Le téléphone sonne", 22/02/06

l'énergie, pour communiquer, on peut pas être tout petit. Généralement les RFID c'est au moins millimétrique. De la même manière le "smart dust", qui sont des objets autonomes ressemblant un peu aux RFID, (…) le "smart dust", la poussière intelligente, c'est millimétrique aussi."

Claude Weisbuch est un scientifique. Aussi est-ce sciemment qu'il ment aux auditeurs de France Inter et leur dissimule ce que son propre institut révèle. Extrait du dossier "La déferlante nano" publié par "*Le journal du CNRS*" en octobre 2005 : "*Outre cet aspect sanitaire, d'autres réflexions d'ordre éthique sont menées sur les conséquences possibles des nanotechnologies sur notre vie quotidienne. Prenons l'exemple des RFID (Radio Frequency Identification Devices), ces étiquettes électroniques déjà utilisées pour identifier nos animaux domestiques, ouvrir et démarrer certaines voitures récentes ou encore suivre à la trace certains produits, de leur fabrication à leur mise en vente. Demain, grâce aux nanotechnologies, ces dispositifs seront amenés à se multiplier dans notre quotidien. Revers de la médaille, ils seront aussi capables de transmettre des informations personnelles sur chacunE* : "Face aux craintes d'atteintes à la vie privée, certains principes généraux ont déjà été suggérés, comme la signalisation claire de leur présence et de leurs caractéristiques, la limitation des données échangées et des possibilités de recoupement ou encore la possibilité de les retirer ou de les inhiber", *analyse Louis Laurent, directeur de département de recherche au CEA et membre de la commission interdisciplinaire "Impacts sociaux et développement des nanotechnologies" du Comité national de la recherche scientifique. Assurément, les nanotechnologies offriront donc la possibilité de fondre les technologies de l'information dans notre environnement. Et l'on parle déjà, par exemple, de poussières électroniques communicantes, minuscules systèmes capables de se mettre en réseau pour recueillir et transmettre des informations.*"

Les nanos sont l'avenir des RFID, pour la raison simple qu'elles permettent d'abaisser le coût unitaire des étiquettes, vers ce fameux plancher de 0,05 € que vise le marché. Essentiellement grâce aux techniques d'impression des antennes par jet d'encre conductrice. "*Nous travaillons avec des vendeurs qui font de l'encre incluant des nanoparticules, permettant d'imprimer les antennes sur le papier moins cher et plus vite", dit Van Fleet, qui fait aussi partie de la direction de R &V Group à Lagrangeville (New York), fabricant de RFID. Une autre société de RFID, Organic ID, à Colorado Spring, travaille sur des antennes imprimées avec des nanoparticules d'or ou d'argent et des polymères.*"[33]

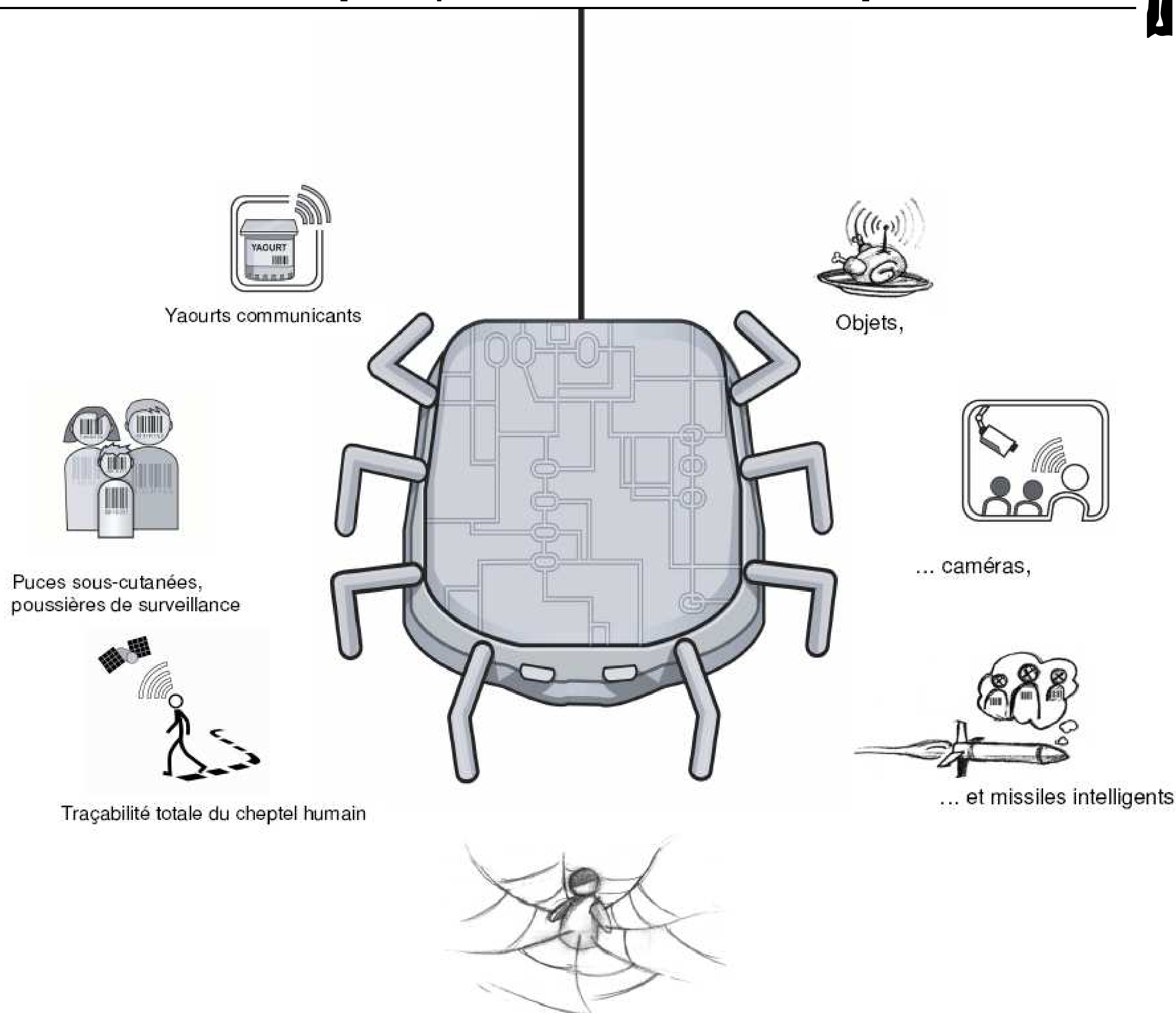
---

33 Traduit de Science Daily, "*Nano will boost RFID tags*", http://www.sciencedaily.com/upi/index.php?feed=Science&article=UPI-1-20050606-14555200-bc-nanoworld-rfid.xml

Si l'on mesure la menace au soin que mettent les chercheurEs à la dissimuler, assurément les RFID méritent notre contestation. Pour commencer, boycottons la carte Avan'Tag des transports technopolitains !

Grenoble, le 7 mars 2006

Pièces et Main d'Œuvre [www.piecesetmaindoeuvre.com]



Pour plus d'infos : http://ogn.ouvaton.org/
Opposition Grenobloise aux Nécrotechnologies

Vers un contrôle social policier sans faille

Paru dans *Silence* n°333, mars 2006

High-tech, sécurité et identification électronique : toutes les techniques sont disponibles pour nous contrôler dans le moindre de nos mouvements. Peut-on arrêter ce "progrès" ?

Une entreprise a breveté le concept UAID (identification unique des adresses) qui permettrait de mettre sous code barre tous les villages, maisons, usines, rues, forêts... à la surface de la planète. Plus besoin de nom de rue, de localité, pour vous adresser un colis. L'UAID est basé sur un code de 22 caractères alphanumérique[34]. L'UAID répondrait ainsi aux besoins des administrations européennes pour la sécurité et la traçabilité des aliments qui s'échangent de manière croissante entre continents et pays. La surface de la planète serait ainsi répertoriée dans un "annuaire" international d'adresses, mise en quelconque sorte sous code barre.
Des systèmes d'identification électronique des produits existent dans l'industrie. Le plus en vogue est le système RFID (identification par fréquence radio)[35] qui permet d'identifier à distance (à travers le carton, le plastique, les murs...), des objets, des animaux, voire... des humainEs.
L'implantation sous-cutanée de ces micro-chips ne semble pas relever de la science-fiction[36], elle est une pratique actuelle. Ce "concept" outre qu'il permet d'accroître la productivité des services de logistiques de tout poil, mais aussi celle de l'élevage et de l'industrie, pourrait bien au bout du compte servir à l'identification des humainEs[37]. Il se trouve en effet que certaines sociétés prônent l'implantation de puces sous la peau de leurs propres salariéEs, ou même de la population. Ce procédé ayant maintenant acquis le vocable l'"empucelage" d'unE individuE, le "dépucelage" correspondrait alors à l'extraction de la puce implantée.
Sans aller aussi loin, la carte d'identité électronique pourrait bien nous réserver des surprises.

Nouvelle carte d'identité : le coercitif à portée de puce

Dans la logique d'un contrôle social toujours plus efficace, pourquoi ne pas faire en sorte que des individuEs puissent être identifiables et repérables géographiquement, à leur insu, en fait de les rendre en quelque sorte "transparentEs" aux yeux du contrôle social.

---

34 Par exemple "32U27C7QDR527SL4Q1K4D"
35 Voir les nombreux sites internet professionnels qui font la promotion de ces puces
36 Voir : http://www.pcinpact.com/actu/news/RFID_une_piqure_dabeille_qui_sauve_la_vie.htm
37 Voir : http://www.verichipcorp.com/

Aujourd'hui, à travers le projet INES (identité nationale électronique sécurisée), l'Etat affiche sa volonté d'imposer à chacunE le principe d'une carte d'identité électronique[38] interrogeable à distance car intégrant une puce RFID, et qui plus est, obligatoire. Il semble bien que ce projet porte atteinte à la protection des individuEs contre l'arbitraire éventuel de la puissance publique, mais aussi aux libertés individuelles tout en réduisant la personne sociale à ses attributs biophysiques.
Tout d'abord, le principe même d'une pièce d'identité dont le port serait obligatoire sont les prémices au déni du principe de liberté de circulation dans l'espace public. Effet, si aux yeux de la société et des institutions unE individuE est en situation irrégulière par le simple fait qu'il ne porte pas sur elle/lui un document (électronique ou non) lui permettant de justifier de son identité, alors cela revient à établir qu'être, en soi, ne suffit plus pour avoir librement sa place dans l'espace public. Faut-il rappeler que de telles dispositions sont, d'abord, l'apanage des dictateurs ? Les pouvoirs publics ont, il y a peu, instauré la gratuité de la carte nationale d'identité. La carte d'identité électronique (obligatoire d'autant qu'elle sera "gratuite") risque fort d'imposer un contrôle social d'une efficacité jamais atteinte dans l'histoire de l'humanité et à l'échelle de la population d'un pays.
Ensuite, le fait que cette "carte d'identité" puisse être interrogeable à distance à l'insu du/de la porteur/euse, constitue une violation de la liberté d'obtempérer, et réduit de fait la population à un cheptel humain[39] qu'il faut gérer de la manière industrielle la plus efficace.

Rappelons que dans le projet INES, il ne s'agit pas de sécuriser la carte d'identité en tant que telle en intégrant dans la puce une sorte de preuve numérique de son authenticité, mais bien d'intégrer dans la puce des informations d'identité et biométriques concernant la/le porteuse/eur[40]. De fait, ce titre d'identité étant électronique réduit cette pièce d'identité à l'état de machine. Ces aspects des choses ont plusieurs conséquences :

- l'information contenue dans le support électronique n'est plus directement et publiquement accessible, donc n'est plus sous le contrôle libre du/de la porteur/euse,
- il est nécessaire de disposer d'un équipement spécifique en bon état de fonctionnement pour pouvoir accéder aux informations du support électronique, équipement qui n'est pas accessible au/à la porteur/euse,
- le fait de rajouter des intermédiaires technologiques à travers la puce elle-

38 Voir le site internet de la Cnil, dossier "titres d'identité" sur http://www.cnil.fr/index.php?id=1773

39 La technique d'identification par puce RFID est déjà en application dans certains élevages bovins

40 Certains pays comme l'Estonie qui a équipé plus de la moitié de sa population, a opté pour une carte avec authentification et signature électroniques, cette carte pouvant servir de ticket de transport, de carte de sécurité sociale et d'accès aux dossiers médicaux, et devrait étendre ses fonctions en incluant le permis de conduire, l'assurance automobile, carte d'électeur (source : http://www.id.ee/ cité par la Direction du programme INES)

même, le programme informatique qui la gère, le système de transmission par radiofréquence, le récepteur qui lit le contenu de la puce à distance... augmente le risque d'erreur voire de malveillance, car au final, ce dispositif est inaccessible à la/au citoyenNE lambda, et obéit aux critères établis par le pouvoir en place,

- alors que le simple fait d'avoir des yeux et de savoir lire étaient les conditions suffisantes pour partager les informations présentes sur la carte d'identité papier, avec la carte d'identité électronique, l'asymétrie entre la/le citoyenNE et les forces de police sera donc singulièrement renforcée.

Contrôle invisible

Mais ce n'est pas tout car, si le port d'une pièce d'identité en France devenait obligatoire sur la voie publique, et si cette pièce était électronique, la connectivité du monde numérique via le Web et le Wap, associée aux possibilités des puces RFID et de l'UAID, ouvrirait sur un monde singulièrement nouveau...

Pour illustrer cette nouveauté voici une situation fictive : vous vous promenez dans la foule en ville et avez en poche votre carte d'identité high-tech, comme il se doit. Vous passez à une vingtaine de mètres d'un représentant des forces de l'ordre. L'agent de la force publique ne vous demande rien puisqu'il/elle peut connaître votre identité en interrogeant à distance les cartes d'identité électronique RFID qui sont à sa proximité, dont la vôtre.

Grâce à la connectivité numérique, il est en mesure de recevoir sur l'écran de son téléphone portable équipé du système d'interrogation des cartes à distance, à la fois votre photo d'identité et les autres renseignements figurant sur votre puce, mais aussi le cas échéant, les autres informations vous concernant que peut lui envoyer un serveur informatique dédié du ministère de l'intérieur.

Dans le même temps, votre positionnement géographique en terme d'UAID (voir plus haut) est associé à votre identification renvoyée par la puce RFID de votre carte d'identité, ceci en temps réel. Ces informations peuvent facilement entrer dans les archives électroniques du dit ministère.

De plus, comme un maillage de balises a été installé sur toutes les grandes villes du territoire, un peu comme pour les relais de téléphones portables (mais avec cette différence que ces balises peuvent être beaucoup plus petites et sont beaucoup plus simples), De la sorte les forces de l'ordre peuvent réaliser un véritable contrôle continu et automatique des déplacements de certaines personnes, voire de leur activité si la carte intègre des fonctions de paiement, de carte de sécurité sociale, de vote... à leur insu. Un tel dispositif permet aussi de contrôler la présence de toutes les personnes qui circulent sur une zone définie comme sensible (un champ d'OGM, une manifestation, une grève...). Vos déplacements géographiques pourront alors être suivis, mémorisés et transférés sur le serveur du ministère de l'intérieur donc accessibles à tous les services de police... de l'espace Schengen, instantanément et surtout automatiquement. Vous êtes fliquéE même si vous ne possédez plus un

portable, car la carte d'identité électronique interrogeable à distance, elle, est obligatoire.

Si vous êtes effectivement recherchéE, le portable de l'agent de la force publique se met à vibrer selon un rythme caractéristique, lui signalant discrètement votre cas, votre visage apparaissant sur son écran. Et si vous n'êtes pas recherchéE : bug informatique ? fausse ressemblance ? erreur de manipulation ? perturbation de la liaison radio ? bouc émissaire idéal ? Autant le dire, la high-tech policière aura forcément les mains sales si on lui donne la possibilité de voir le jour.
Enfin, précisons que certainEs tenantEs de ces techno-folies prônent l'implantation dans le corps, par exemple dans une des deux mains, entre les os du métacarpe, son implantation étant ici facile et son extraction ne pouvant être que volontaire, car nettement plus difficile.
Futur improbable ? Allégations sans fondements ? Observons tout de même que les banques adoptent le RFID. Par exemple Visa, après Master Card et American Express, se dotent d'une carte de paiement RFID[41]. Qui refusera une carte de crédit qu'il n'est même plus besoin de sortir de sa poche ? Les occasions de préparer les masses au "concept" RFID sont nombreuses comme l'ont précisé les auteurs de Pièces et main d'oeuvre[42].

Des moyens efficaces, des fichiers peu fiables
Le pouvoir en place a déjà préparé le terrain technique, judiciaire et médiatique depuis des années pour un flicage technologique idéal. Il s'est doté de réseaux de communication, de fichiers et de matériels spécifiques et compatibles[43], il a modifié la loi informatique et libertés durant l'été 2004, accordant des libertés inédites aux organes ayant la responsabilité du fichage des citoyenNEs, ce que la Commission nationale informatique et libertés a clairement critiqué[44]. Rien d'illogique à ce qu'aujourd'hui il soit en train de vanter les mérites d'une carte d'identité à puce basée sur la biométrie, comptant sur le "sentiment d'insécurité", sensé crédibiliser la nécessité du renforcement du contrôle social.
La France excelle dans la création de fichiers dont les grosseurs ne posent plus de problème d'utilisation avec l'informatique embarquée et les réseaux de télécommunication. Par contre, la multiplicité de ces fichiers officiels ou

41 Voir : http://solutions.journaldunet.com/0503/050201_visa_rfid.shtml
42 Téléphone portable, gadget de destruction massive, Silence n°328 et 329
Disponible aussi en version brochure, voir : http://infokiosques.net/spip.php?article=267
43 La compatibilité technique des fichiers et des matériels n'est pas un problème, les technologies de l'information mises en oeuvre concernant la sécurité sont maintenant conçues de manière à atteindre une versatilité maximale
44 Voir la position de la Cnil sur www.cnil.fr/fileadmin/documents/approfondir/dossier/CNIbiometrie/Position-cnil-CNI-05-2005.pdf

devenus officiels[45], s'ajoute à la pratique des "listes noires"[46], ainsi qu'à la qualité[47] et la fiabilité[48] très discutées contenues dans ces fichiers.
Mais, au-delà de ces faits graves, c'est surtout la compatibilité de l'existence et de l'usage de ces réseaux, fichiers et matériels, avec les droits et libertés humains qui pose problème.
En effet, le refus d'un contrôle d'identité à lui seul peut justifier une inscription au fichier STIC, le refus de se soumettre à un prélèvement afin d'être intégréE dans un fichier tel que le fichier FNAEG peut se révéler être une infraction pouvant impliquer une inscription au fichier STIC[49]. On rappellera juste qu'au Royaume-Uni, vous ne pouvez pas vous faire reprocher par la force publique de ne pas avoir de carte d'identité, car, de haute lutte au sein des institutions politiques de ce pays, il n'y a toujours pas, pour l'instant, de carte d'identité au pays de Shakespeare.

18 La voie du progrès et de la sécurité est pavée de bonnes intentions



"Mais quel esprit torturé avez-vous ! L'unification des systèmes tels que l'UAID et le RFID, vous permettra de vivre avec moins de soucis. Plus besoin de code pour votre carte bancaire, ni même besoin de la sortir de votre poche, plus besoin de clefs pour ouvrir la porte du domicile, et en cas d'accident, la puce contiendra les informations de base informant les secouristes de vos particularités médicales".

Pour la quiétude de la/du citoyenNE consommateur/trice sécuriséE, toute mobilité pourra être repérée, tout rapprochement de deux individuEs dans une même zone ou deux zones proches pourra être identifié, analysé, mémorisé.

---

45 On citera par exemple : FICP (fichier national des incidents de remboursement des crédits aux particuliers), RNIPP (répertoire national d'identification des personnes physiques), FCA (fichier central des automobiles), FAED (fichier automatisé des empreintes digitales), AGDREF (application de gestion des dossiers des ressortissants étrangers en France), STIC (système de traitement des infractions constatées), Judex (fichier propre à la gendarmerie nationale), FNAEG (fichier national des empreintes génétiques), OFPRA (fichiers de l'Office français de protection des réfugiés et apatrides), FPR (fichier des personnes recherchées), FNI (fichier national des immatriculations), RNIAM (répertoire national interrégimes des bénéficiaires de l'assurance maladie), Preventel (base de prévention des impayés), Europol (fichier de la "police" européenne), SIS (système d'information Schengen)...

46 Voir le dossier de la Cnil proposé au téléchargement sur son site http://www.cnil.fr/index.php?id=1000

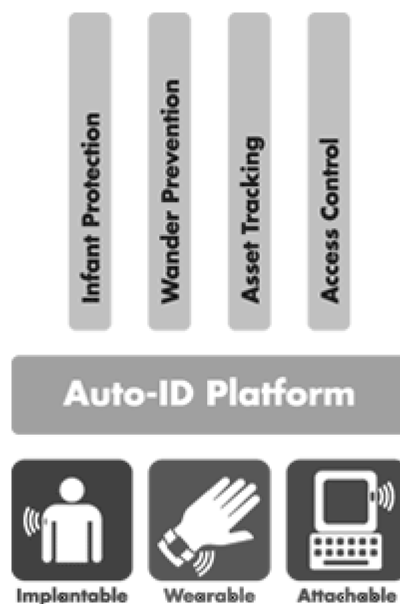
47 Des informations relevant de la vie privée, à caractère racial, sexuel ou politique sont souvent constatées par la Cnil elle-même (voir les descriptifs des fichiers sur le site de la Cnil, dossier "Fichiers en Fiches")

48 Par exemple concernant le fichier "Stic", la Cnil a constaté un taux d'erreur de 25% (source Cnil)

49 Source : Cnil

Certains clameront l'impossible mariage entre liberté et sécurité. "Mais cher monsieur, foin de telles paroles de Cassandre, vivez avec votre temps que Diable, on arrête pas le progrès ! ".
Et on vous expliquera que si telle personne, enlevée par un maniaque avait eu une puce RFID sur elle, voire implantée en elle (c'est plus sûr), on aurait pu la retrouver aisément avant que le pire n'arrive... On a bien entendu des discours semblables dans certaines affaires, cette fois à la faveur des téléphones portables.
1984 et *Le meilleur des mondes* semblent peu à peu prendre corps dans le présent. Mais n'y sommes-nous pas déjà un peu préparéEs, voire un peu consentantEs ? Un collège californien[50] a imposé aux élèves, sans demander l'avis à leurs parents, de porter des badges RFID, afin d'automatiser donc faciliter l'intendance de l'établissement, le contrôle des absences, mais aussi réduire le vandalisme, car pouvant de la sorte localiser et retrouver tous les déplacements horodatés de chaque étudiantE dans l'établissement...
Pour éviter de telles dérives sécuritaires, donc rejeter un état civil biométrico-radiosécurisé et conserver un état civil simplement social[51] avec si désiré une carte d'identité en papier avec à la rigueur des hologrammes incorporés, il faudra certainement lutter. Dans les faits, de plus en plus de pays européens s'apprêtent à adopter des techniques semblables, et les institutions européennes n'y voient aucun inconvénient... Alors, le flicage numérique high-tech, qui veut vivre avec ?

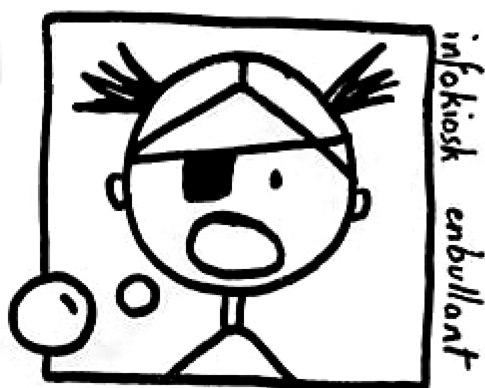
Daniel Julien



50 Voir : http://www.incomcorporation.com/ et http://www.principalspartnership.com/idbadges.pdf
51 Rappelons que l'existence de la carte d'identité est considérée dans un certain nombre de pays comme une mesure liberticide, et que cette mesure est, en France, un héritage particulier complètement intégré dans nos moeurs

Nous avons rassemblé, féminisé, arrangé deux textes qui permettent d'articuler la critique des nanotechnologies aux politiques sécuritaires qui font la gloire et la fortune de quelques gouvernantEs et industrielLEs, au détriment de nos libertés d'aller et venir, de se rassembler, de penser différemment.

N'hésitez pas à nous contacter pour nous envoyer vos commentaires.



Pour plus d'infos :
http://infokioskenbullant.c.la/
Pour nous contacter :
infokioskenbullant@no-log.org